

CLAIMS

1. An information recording medium manufacturing method, comprising:

a scramble rule acquiring step for acquiring a scramble rule to apply to the content to be recorded on the information recording medium;

a scrambling processing step for executing the scrambling processing as to the content, according to the scramble rule acquired in said scramble rule acquiring step; and

a step for recording the scrambled content generated in said scrambling processing step and the scramble rule applied to the content, onto an information recording medium.

2. An information recording medium manufacturing method according to Claim 1, wherein said scramble rule acquiring step is a step for acquiring individual scramble rules for each recording content or for each management unit, in the event of a plurality of content to be recorded to the information recording medium.

3. An information recording medium manufacturing method according to Claim 1, wherein said scrambling processing step is a step for performing processing to replace at least

one portion of the content data to be recorded to said information recording medium;

and wherein said scramble rule includes data which points to the position to which the content data is to be replaced.

4. An information recording medium manufacturing method according to Claim 1, wherein the scrambling processing executed in said scrambling processing step is shuffling processing of shuffle elements which are set as content-comprising data;

and wherein said scramble rule is data which describes the shuffle state of said shuffle elements.

5. An information recording medium manufacturing method according to Claim 1, wherein the scrambling processing executed in said scrambling processing step is Exclusive-OR computing processing of the content-comprising data and a previously set settings value or a value calculated based on this settings value;

and wherein said scramble rule is data describing said settings value.

6. An information recording medium manufacturing method according to Claim 1,

wherein the scrambling processing executed in said scrambling processing step is a rotating processing of the content-comprising data;

and wherein said scramble rule is data describing a shift amount in the rotation.

7. An information recording medium manufacturing method according to Claim 1, further comprising an encrypting processing step for executing encrypting processing of the recorded content of the information recording medium, after executing said scrambling processing step, or before executing the same.

8. An information recording medium manufacturing method according to Claim 7,

wherein the scrambling processing executed in said scrambling processing step is a shuffling processing of the shuffled elements which are set as content-comprising data;

and wherein the encrypting processing executed in said encrypting processing step is encrypting processing in CBC mode executed on data units the same size as that of said shuffled elements.

9. An information recording medium manufacturing method according to Claim 1, wherein the data for processing which

is executed in the scrambling processing in said scrambling processing step is data which includes at least one of the following:

- (1) a portion of I-picture slice encoded data included in the MPEG encoded data,
- (2) a portion of the sequence header, and
- (3) PID data storing the data-type information within the transport stream packet.

10. An information processing device for executing content recording processing as to the information recording medium, comprising:

a scrambling processing unit for acquiring a scramble rule to be applied to the content to be recorded on the information recording medium, according to the acquired scramble rule; and

a recording processing unit for recording the scrambled content generated in said scrambling processing unit, and the scramble rule applied to this content, to the information recording medium.

11. An information processing device according to Claim 10, wherein said scrambling processing unit has a configuration for acquiring individual scramble rules for each recording content or for each management unit, in the

event of a plurality of content to be recorded to the information recording medium, and executing scrambling processing for each content according to the acquired scramble rule.

12. An information processing device according to Claim 10, wherein said scrambling processing unit has a configuration for performing processing to replace at least one portion of the content data to be recorded to said information recording medium;

and wherein said scramble rule includes data which points to the position to which the content data is to be replaced.

13. An information processing device according to Claim 10, wherein the scrambling processing executed in said scrambling processing unit is shuffling processing of shuffle elements which are set as content-comprising data;

and wherein said scramble rule is data which describes the shuffle state of said shuffle elements.

14. An information processing device according to Claim 10, wherein the scrambling processing executed in said scrambling processing unit is Exclusive-OR computing processing of the content-comprising data and the previously

set settings value or a value calculated based on this settings value;

and wherein said scramble rule is data describing said settings value.

15. An information processing device according to Claim 10, wherein the scrambling processing executed in said scrambling processing unit is a rotating processing of the content-comprising data;

and wherein said scramble rule is data describing a shift amount in the rotation.

16. An information processing device according to Claim 10, further comprising an encrypting processing unit for executing encrypting processing of the recorded content of the information recording medium.

17. An information processing device according to Claim 16, wherein the scrambling processing executed in said scrambling processing unit is a shuffling processing of the shuffled elements which are set as content-comprising data;

and wherein the encrypting processing executed in said encrypting processing unit is encrypting processing in CBC mode executed on data units the same size as that of said shuffled elements.

18. An information processing device according to Claim 10, wherein

said scrambling processing unit is data for scrambling processing which includes at least one of the following:

(1) a portion of I-picture slice encoded data included in the MPEG encoded data,

(2) a portion of the sequence header, and

(3) PID data storing the data-type information within the transport stream packet.

19. An information processing device for executing playback processing of the content recorded on the information recording medium, comprising:

a scrambling processing unit for executing descrambling processing of the content recorded on the information recording medium; wherein

said scrambling processing unit executes analyzing of the scramble rule which is the scrambling processing information corresponding to the content stored in said information recording medium, and from the results of the deciphering, executes descrambling processing to the scramble rule for each of the acquired individual content.

20. An information processing device according to Claim

19, wherein said scrambling processing unit has a configuration for acquiring individual scramble rules for each recording content or for each management unit, in the event of a plurality of content to be recorded to the information recording medium, and executing descrambling processing for each content according to the acquired scramble rule.

21. An information processing device according to Claim 19, wherein said scrambling processing unit has a configuration for performing processing to replace at least one portion of the content data to be recorded to said information recording medium;

and acquires the position data for pointing to the position to which the acquired content data is replaced from the results of analyzing said scramble rule, and based on this position data, executes descrambling processing.

22. An information processing device according to Claim 19, wherein said descrambling processing executed with said scrambling processing unit is processing for restoring the shuffle state of the shuffle elements which are set as content-comprising data;

and wherein said scramble rule is data describing the shuffle state of said shuffle elements;



and wherein said scramble processing unit executes shuffle state restoring processing of the shuffle elements based on said scramble rule.

23. An information processing device according to Claim 19, wherein said descrambling processing executed with said scrambling processing unit is Exclusive-OR computing processing of the content-comprising data and the previously set settings value or a value calculated based on this settings value;

and wherein said scramble rule is data describing said settings value;

and wherein said scramble processing unit executes Exclusive-OR computing processing of the content-comprising data and the previously set settings value based on said scramble rule.

24. An information processing device according to Claim 19, wherein said descrambling processing executed with said scrambling processing unit is rotation processing for the content-comprising data;

and wherein said scramble rule is data describing the shift amount in the rotation;

and wherein said scramble processing unit executes rotation restoring processing based on said shift amount,

based on said scramble rule.

25. An information processing device according to Claim 19, wherein said information processing device further comprises an encrypting processing unit for executing decrypting processing of the recorded content of the information recording medium.

26. An information processing device according to Claim 25, wherein said scrambling processing executed in said scrambling processing units is shuffling processing of the shuffle elements which are set as content-comprising data; and wherein the decrypting processing executed in said encrypting processing units is decrypting processing in CBC mode which executed on data units the same size as that of said shuffled elements.

27. An information processing device according to Claim 19, wherein said scrambling processing unit is data for descrambling processing which acquires data including at least one of the following and executing processing thereof:

- (1) a portion of I-picture slice encoded data included in the MPEG encoded data,
- (2) a portion of the sequence header, and
- (3) PID data storing the data-type information within

the transport stream packet.

28. An information recording medium for storing:  
recorded data as scrambled content having scrambling processing executed according to a scramble rule set for each recording content or for every management unit; and  
the scramble rule applied to said scrambled content.

29. An information recording medium according to Claim 28, wherein said scrambling processing is processing for replacing at least one portion of said content;  
and wherein said scramble rule is a rule for recording the data showing the position of the portion of data of said content data to be replaced.

30. An information recording medium according to Claim 28, wherein said scrambled content is scrambled content generated by the shuffling processing of the shuffle element set as the content-comprising data;  
and wherein said scramble rule is data describing the shuffle state of said shuffle elements.

31. An information recording medium according to Claim 28, wherein said scrambled content is scrambled content generated by EXOR computing processing of the content-

comprising data and the previously set settings value or a value calculated based on this settings value;

and wherein said scramble rule is data describing said settings value.

32. An information recording medium according to Claim 28, wherein said scrambled content is scrambled content generated by rotation processing of the content-comprising data;

and wherein said scramble rule is data describing a shift amount in the rotation.

33. An information recording medium according to Claim 28, wherein said scrambled content is scrambled content generated by shuffling processing of the shuffle elements which as set as content-comprising data;

and wherein said information recording medium has the configuration to record content encrypted by the encrypting processing in CBC mode which executes with data the same size as that of said shuffled elements as a unit.

34. An information processing device according to Claim 28, having a configuration wherein said scrambled content includes as scrambling processing data at least one of the following:

- (1) a portion of I-picture slice encoded data included in the MPEG encoded data,
- (2) a portion of the sequence header, and
- (3) PID data storing the data-type information within the transport stream packet.

35. An information processing method for executing content recording processing to an information recording medium, said method comprising:

- a scramble rule acquiring step for acquiring a scramble rule to apply to the content to be recorded on the information recording medium;

- a scrambling processing step for executing the scrambling processing as to the content, according to the scramble rule acquired in said scramble rule acquiring step;
- and

- a step for recording the scrambled content generated in said scrambling processing step and the scramble rule applied to the content, onto an information recording medium.

36. An information processing method for executing playback processing of the content recorded on an information recording medium, said method comprising:

- a scrambling processing step for executing descrambling processing of the content recorded on the information

recording medium; wherein

said scrambling processing step further has a scramble rule analyzing step for executing analyzing of the scramble rule which is the scrambling processing information corresponding to the content stored in said information recording medium, and a descrambling step for, based on the results of said scramble rule analyzing step, executing descrambling processing corresponding to the scramble rule for the acquired individual content.

37. A computer program for executing content recording processing to an information recording medium with a computer, said program comprising:

a scramble rule acquiring step for acquiring a scramble rule to apply to the content to be recorded on the information recording medium;

a scrambling processing step for executing the scrambling processing as to the content, according to the scramble rule acquired in said scramble rule acquiring step; and

a step for recording the scrambled content generated in said scrambling processing step and the scramble rule applied to the content, onto an information recording medium.

38. A computer program for executing playback processing

of the content recorded on the information recording medium with a computer, said program comprising:

a scrambling processing step for executing descrambling processing of the content recorded on the information recording medium; wherein

said scrambling processing step further comprises a scramble rule analyzing step for executing analyzing of the scramble rule which is the scrambling processing information corresponding to the content stored in said information recording medium, and a descrambling step for, based on the results of said scramble rule analyzing step, executing descrambling processing corresponding to the scramble rule for the acquired individual content.